**Microsoft LAPS - How to Implement Securely**

**Install the LAPS Management Utilities**

* Download the LAPS Installer(s) to a domain joined computer
* #invoke-webrequest -uri "https://www.microsoft.com/en-us/download/confirmation.aspx?id=46899&6B49FDFB-8E5B-4B07-BC31-15695C5A2143=1" -outfile c:\temp\lapsx64.msi
* #msiexec /i c:\temp\LAPSx64.msi

**Extend the Act**m**ive Directory Schema**

Import-Module AdmPwd.PS

Update-AdPwdADSchema

Will add 2 properties in AD when finished

ms-Mcs-AdmPwd – This attribute stores the local administrator password

ms-Mcs-AdmPwdExpirationTime – This attribute stores the password expiration time

**Configure Active Directory Computer Permissions**

* Get OU structure
* (get-adorganizationalunit -filter \* properties \*).distinguishedname
* Set-AdmPwdComputerSelfPermission -Identity "OU Name"

**Configure Active Directory User Permissions**

* Set-AdmPwdReadPasswordPermission –Identity "OU Name" –AllowedPrincipals "User or Group Name"

**Delegate rights to an AD user or Group to modify the reset time attribute**

* Set-AdmPwdResetPasswordPermission –Identity "OU Name" -AllowedPrincipals "User or Group Name"

By default, The specified group you delegated permissions to, NT AUTHORITY\SYSTEM, and Domain Admins should be listed as extended right holders. If there are any other users or groups listed under the ExtendedRightHolders property, these could be users or groups that unintentionally have access to view the attributes. Make sure any unwanted users/groups are removed from extended rights To do this go to ADUC and:

1. Right click on the OU in question and select Properties

2. Click on the Security tab

3. Click Advanced

4. Select the user or group to modify permissions for

5. Click Edit

6. Uncheck the All extended rights box

In order for the local administrator password to be randomized on devices, two conditions need to be met.

1. The client needs to have a group policy object linked that enables LAPS

2. The client needs to have the LAPS group policy client-side extensions installed so it knows what LAPS is

**Configure Group Policy to Deploy LAPS Settings**

Install the LAPS Group Policy Administrative Template

* Group policy does not natively know about the LAPS settings. The settings need to be pulled from an administrative template.
* From the computer where the LAPS management utilities were installed and copy the policy templates to AD Central Store
* copy C:\Windows\PolicyDefinitions\admpwd.admx \\domain.fqdn\SYSVOL\domain.fqdn\Policies\PolicyDefinitions
* copy C:\Windows\PolicyDefinitions\en-US\AdmPwd.adml \\domain.fqdn\SYSVOL\domain.fqdn\Policies\PolicyDefinitions\En-us

**Create a Group Policy Object to Deploy LAPS Settings**

1. Group Policy Management Console

2. Right click on the Group Policy Objects folder and select New

3. Name the policy and click OK (In this example the policy is named LAPS)

4. Right click on the newly created policy and select Edit

5. Go to Computer Configuration > Policies > Administrative Templates > LAPS (There are 4 settings available)

* Enable local admin password management – Enabled
* Password Settings – Enabled
* Do not allow password expiration time longer than required by policy - Optional but recommended
* Name of administrator account to manage –

6. Once the settings have been configured, Right click the OU that you to assign LAPS to

**LAPS and password storage in clear text in AD (How it should be protected)**

-Permission to read the password from AD be sure to remove all users/groups from the extended rights attributes earlier

-Only use tools that protect the information in traffic and protections can not be enforced on the server side, it must be initiated by the client By default LAPS uses kerberos type of encryption during transport, Both LAPS UI and Powershell uses this protection

**Other tools**

LDP.exe offers the option to use encrypted connection by default but if you know what you're doing you can still connect unencrypted

ADSI - can reveal the password through unencrypted queries, with ADSI you shoudl always use IADsOpenDSObject interface and specify USE\_SIGNING and USE\_SEALING in OpenDSObject method

AD Powershell - is protected. get-ADcomputer uses ADWS instead of LDAP

.NET Framework - Encryption needs to be turned on for all LDAPConnections. implement LDAPs. And enforce use of LDAPs with group policy

RODCs = ms-Mcs-AdmPwd attribute is flagged not to be replicated to RODCs